UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MALIBU MEDIA, LLC,	:	
	:	Case No. 1:15-cv-10133-RA
Plaintiff,	:	
	:	Judge Abrams
vs.	:	
JOHN DOE subscriber assigned IP address 24.90.48.223,	:	
Defendant.	:	

DECLARATION OF PATRICK PAIGE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE

[Remainder of page intentionally left blank]

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. From 1989 until 2011 I was employed by the Palm Beach County Sherriff's Department. For eleven years, from 2000 to 2011, I served as a detective in the Computer Crimes Unit.

3. As a part of my duties within the Computer Crimes Unit, I investigated cases involving the use of the Internet, including cases involving peer-to-peer file sharing networks.

4. I have conducted forensic computer examinations for:

   a. Broward County Sheriff's Office;

   b. Federal Bureau of Investigations;

   c. U.S. Customs and Border Patrol;

   d. Florida Department of Law Enforcement;

   e. U.S. Secret Service;

   f. Bureau of Alcohol, Tobacco, Firearms and Explosives; and

   g. Various municipalities in the jurisdiction of Palm Beach County.

5. I was assigned to a police unit working in conjunction with TLO Corp., which is a private company. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which consisted of six online investigators and two computer forensics examiners.

6. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with

persons who were sending sexually explicit photographic images of children or other illegal content over the Internet using peer-to-peer file sharing programs.

7. I have received the following awards and commendations:

a. 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.

b. 1997 – Deputy of the Month for June.

c. 2001 – Detective of the Month for October.

d. 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.

e. 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.

f. 2005 – Detective of the Month for December.

g. 2006 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.

h. 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

8. I have taken over 400 hours of courses designed to teach people how to investigate computers.

9. I have also taught over 375 hours of courses instructing various personnel in computer forensics. I have instructed students from various government branches, including:

a. sheriff's offices;

b. FBI agents;

c. ATF agents;

d. agents from the Central Intelligence Agency; and

e. individuals from other branches of government and the private sector.

10. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics before state, federal, and military courts in California, Florida, Indiana, New Jersey, New York, and Pennsylvania.

11. After leaving the Palm Beach County Sherriff's office, I founded Computer Forensics, LLC, where I am currently employed. In my current position, I have served as an expert witness in several of Malibu Media, LLC's cases.

12. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets.

13. Through my work experience, I have obtained direct and firsthand knowledge regarding the methods the government and copyright holders use to investigate and identify cyber criminals and copyright infringers. During the initial phase of Internet-based investigations, an offender's IP address, as well as the date and time of the illegal transmission, is recorded. The offender is only known by an IP address.

14. In my professional experience, investigations into unlawful internet activity through the use of an IP address involve subpoenaing an Internet Service Provider to identify the internet subscriber assigned the IP address associated with the unlawful internet activity. When the only evidence of a cybercriminal or online copyright infringer's identity is a recording of an illegal or infringing computer transaction, law enforcement and copyright holders *must* subpoena Internet Service Providers because without the information identifying the subscriber of the IP address, they are unable to otherwise identify an anonymous internet subscriber. Both the police and copyright owners routinely use this process.

15. My experience teaches me that the ***only*** entity able to correlate an IP address to a specific individual at a given date and time is the Internet Service Provider. And, through my

tenure with the Palm Beach County Sheriff's Office and while working with TLO Corp., I learned that Internet Service Providers will not disclose the identities of subscribers to whom IP addresses are assigned without a subpoena.

16. In the investigations in which I have been involved, the subpoenaing party has only been able to learn the identity of the subscriber after, (a) issuing a subpoena to the Internet Service Provider, and (b) the Internet Service Provider uses its subscriber logs to identify the subscriber in control of an IP address at a specific date and time.

17. In the criminal context, I have been directly involved in the execution of approximately 200 search warrants either by way of managing the process or performing it personally. A law enforcement officer would request that the assistant state attorney subpoena the corresponding Internet Service Provider for the purpose of identifying the subscriber, and the subscriber would not be notified by the Internet Service Provider that his or her identity was being subpoenaed (because such notice would allow the subscriber to destroy evidence, delete the images, and destroy the data).

18. During my time in the Computer Crimes Unit, I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the alleged illegal activity at the dwelling identified in the search warrant. In that one instance, the Wi-Fi connection was not password protected, and the offender was actually a neighbor behind the subscriber's residence.

19. I have never come across a Wi-Fi hacker situation and, in my opinion, a child pornographer has a greater incentive to hack someone else's Wi-Fi connection than a BitTorrent user or copyright infringer because transmission of child pornography is a various serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

20. The process used by law enforcement to detect cyber criminals mirrors the process used by Malibu Media, LLP to detect copyright infringers.

21. Malibu Media, LLP uses an infringement detection system that is owned by Excipio GmbH ("Excipio") and licensed by IPP International UG ("IPP"), with whom Malibu Media, LLC has contracted. I tested this infringement detection system, and IPP provided me with information throughout the testing process.

22. To test Excipio's infringement detection system, I downloaded four public domain movies from the national archive.

23. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

24. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP address.

25. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client—the software that enables the BitTorrent protocol to work—onto each server.

26. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which Excipio uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

27. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

28. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

29. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

30. The screen captures sent by IPP had my codes on them; thus, I knew that Excipio's infringement detection system had caught the movies I had seeded.

31. IPP also sent me additional data identifying the IP address used by each of the four servers, and sent me PCAPs.

32. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs matched my PCAPs. This could not have happened unless Excipio's server was connected to the test server because the transactions would not match. From this test, I concluded that Excipio's infringement detection system works, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

33. Aside from this test, in Malibu Media, LLC's infringement cases, I have reviewed the deposition transcripts of Internet Service Providers' 30(b)(6) representatives. In each deposition I reviewed, the witness testified that he was "certain" the Internet Service Provider had correctly correlated the IP address to the correct subscriber.

34. Based on my personal experience, I have confirmed that Malibu Media, LLC is able to accurately identify its copyright infringers by subpoenaing the responsible Internet Service Providers. I have performed numerous computer forensics examinations for Malibu Media, LLC, and I have routinely found either (1) evidence of copyright infringement of Malibu Media, LLC's works or (2) evidence of suppression and spoliation. By way of illustration only, I discuss a few examples:

a. *Malibu Media, LLC v. Weaver*, No. 8:14-cv-01580-VMC-TBM (M.D. Fla. 2015): I was able to locate evidence that almost all of Malibu Media, LLC's infringed works had once existed on the IP registrant's computer. Further, prior to

producing his hard drive for examination, the IP registrant deleted evidence of the works. . I am in the processing of finalizing my expert report for this matter.

b. *Malibu Media, LLC v. John Doe*, No. 1:14-cv-10155-KBF (S.D.N.Y. 2015): Forensic examination that the IP registrant had eleven different file destruction software on his hard drive – each with the capability of destroying substantial amounts of data - on. Further, I discovered that he *used* one of the software on his hard drive just days before turning it over for imaging and examination. The spoliation on his hard drive was so extensive that it contained only one instance of the IP registrant's name; and that one instance proved that the IP registrant had failed to disclose and produce another electronic device. I also detected that prior to Defendant's use of the file destruction software, the IP registrant had connected another undisclosed external storage device to his hard drive. This suggested that the individual was storing certain data which he wanted to retain.

c. *Malibu Media, LLC v. Harrison*, No. 1:12-cv-01117-WTL-MJD (S.D. Ind. 2015): I discovered that the IP registrant had six network storage devices which he failed to disclose or produce. Further examination revealed that through the IP registrant's use of a Local Area Network, he used his laptop computer to access and retrieve files stored on the undisclosed network storage devices. Significantly, I was able to confirm that many of the files stored on the undisclosed network storage devices were files that the IP registrant had downloaded using BitTorrent.

d. *Malibu Media, LLC v. Tashiro*, No. 1:13-cv-00205-WTL-MJD (S.D. Ind. 2014): I discovered that the IP registrant and her husband failed to disclose and produce numerous computer devices, and had committed demonstrable perjury. The undisclosed devices included an external hard drive which the defendant's expert examined prior to its disclosure, and a large desktop computer. Of the computer devices I examined, I located extensive evidence of illegal BitTorrent use.

e. *Malibu Media, LLC v. Huseman*, No. 1:13-cv-02695-WYD-MEH (D. Colo. 2014): I was able to uncover remnants of torrent files and Malibu Media LLC's copyrighted works in the unallocated space of the IP registrant's computer hard drive. The evidence conclusively established that the IP registrant had downloaded Malibu Media LLC's films, and attempted to destroy evidence of his infringement.

f. *Malibu Media, LLC v. John Doe*, No. 12-2078 (E.D. Pa. 2013): In this "Bellwether" case, wherein Malibu Media, LLC won the first ever BitTorrent copyright infringement trial, I located computer evidence which conclusively established that the IP registrant had reformatted or "wiped" his hard drive and reinstalled the operating system in order to conceal evidence of the infringements. This evidence proved that the IP registrant had testified falsely at trial.

35. The foregoing is a small sampling of the examinations I have conducted. These and all of the other examinations I have conducted lead me to reasonably believe: (1) that Excipio obtains and Malibu Media, LLC accurately identifies the IP addresses that are infringing its copyrighted works; (2) that Malibu Media, LLC, just like law enforcement, must subpoena Internet Service Providers in order to identify who controls the internet connections being used to infringe its copyrighted works; and (3) that without the identity of the responsible IP registrant, Malibu Media, LLC cannot prove its copyright infringement claims.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 27th day of October, 2015.

PATRICK PAIGE

By: